UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,365	07/03/2001	Teng Pin Poo	1601457-0007	4356

7470 7590 08/01/2008

WHITE & CASE LLP
PATENT DEPARTMENT
1155 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
08/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/898,365
Filing Date: July 03, 2001
Appellant(s): POO ET AL.

Warren S. Heit
Reg. No. 36,828
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 3/20/08 appealing from the Office action mailed 2/20/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6088802	Bialick	7-2000
6799275	Bjorn	9-2004
6385667	Estakhri	5-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 1, 2, 4, 5, 7, 8,10, 11, 13-14, 17, 18 and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Bialick et al. United States Letters Patent No. 6,088,802.

As per claim 1:

Bialick et al. teach a portable device comprising:

a microprocessor; and (Figure 8, item 801)

a non-volatile memory coupled to the microprocessor; (Figure 8, item 803; Col. 16, lines 10-16) and

a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise. (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

As per claim 2:

The rejection of claim 1 is incorporated and further Bialick et al. disclose the biometrics-based authentication module is a fingerprint authentication module. (Col. 14, lines 26-28)

As per claim 4:

The rejection of claim 1 is incorporated and further Bialick et al. disclose the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device. (Col. 14, lines 48-49; Col. 14, line 59-Col. 15, line 7)

As per claim 5:

The rejection of claim 1 is incorporated and further Bialick et al. disclose a non-volatile memory capable or storing biometrics information usable for authentication. (Figure 8, item 803; Col. 14, lines 57-58; Col. 16; lines 10-11)

As per claim 7:

Bialick et al. disclose a portable device comprising:

a bus; (Figure 6, item 609)

a microprocessor coupled to the bus; (Figure 8, item 801)

a non-volatile memory coupled to the bus (Figure 8, item 803; Col. 16, lines 10-15); and

a biometrics-based authentication module coupled to the bus, wherein under the control of the microprocessor the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (Col. 14, lines 55-56) (2) store the first biometrics marker in the non-volatile memory; (Col. 14; lines 57-58) (3) capture a second biometrics marker; (Col.14; line 54) and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker; (Col.14; line 54)and wherein microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module. (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

As per claim 8:

The rejection of claim 7 is incorporated and further Bialick et al. disclose the biometrics-based authentication module is a fingerprint authentication module. (Col. 14, lines 26-28)

As per claim 10:

The rejection of claim 7 is incorporated and further Bialick et al. disclose the biometrics-based authentication module is structurally integrated with the portable device in a unitary construction and comprises a biometrics sensor being disposed on one surface of the portable device. (Col. 14, lines 48-49; Col. 14, line 59-Col. 15, line 7)

As per claim 11:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a portable device, wherein the non-volatile memory comprises flash memory. (Figure 8, item 803)

As per claim 13:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a portable device, wherein the microprocessor is configured to direct the biometrics-based authentication module to capture and store the first biometrics marker provided that no biometrics marker has been stored in the non-volatile memory. (Col. 14, lines 55-58)

As per claim 14:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a portable device, wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module. (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

As per claim 17:

Bialick et al. teach a biometrics-based authentication method implemented using a portable device, the method comprising the steps of: (a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device; (Col.14; line 54) (b) retrieving a registered biometrics marker from a non-volatile memory of the portable device, the registered biometrics marker having been stored therein during a registration process; (Col. 14; lines 57-58) (c) comparing the first biometrics marker against the registered biometrics marker; (Col. 14; lines 54-56) (d) denying the user access to the non-volatile memory provided that a match is not identified in said step (c); (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16) (e) signaling an authentication success provided that a match is identified in said step (c). (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

As per claim 18:

The rejection of claim 17 is incorporated and further Bialick et al. disclose biometrics-based access control method, wherein the registered biometrics marker is a fingerprint. (Col. 14, lines 26-28)

As per claim 20:

The rejection of claim 17 is incorporated and further Bialick et al. disclose the step of denying the user access to the restricted resource provided that a match is not identified in said step (c). (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Appellant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 6, 12, 16, 19 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. United States Letters Patent No. 6,088,802.

As per claim 6:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick et al. is that, the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module. However, it would have been

obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include a microprocessor that is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

As per claim 12:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to enhance the security of the biometrics-based access control method.

As per claim 16:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick et al. is that, a bypass mechanism

for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include a bypass mechanism for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

As per claim 19:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device can be used to encrypt or decrypt data stored. Not explicitly disclosed by Bialick et al. is that, the registered biometrics marker is stored in an encrypted format.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include the registered biometrics marker is stored in an encrypted format. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to enhance the security of the biometrics-based access control method.

As per claim 22:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device driver can be implemented so that the user must successfully enter an

acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick et al. is that, providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include providing the user with a bypass authentication procedure provided that a match is not identified in said step (c). This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

4. Claims 3 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. United States Letters Patent No. 6,088,802 and in view of Bjorn United States Letters Patent No. 6,799,275 .

As per claim 3:

Bialick et al. teach all the subject matter as described above. In addition, Bialick et al. disclose a communication interfaces, such as a smart card interface, a serial interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick et al. is that the portable device, further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device.

Bjorn in analogous art, however, teaches a device further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device. (Col. 2, lines 59-60; the digital connection is a data bus, which conforms to a universal serial bus (USB) standard.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick et al. to include a device further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Bjorn, in order to provide a faster transfer of digitized image.

As per claim 9:

Bialick et al. teach all the subject matter as described above. In addition, Bialick et al. disclose a communication interfaces, such as a smart card interface, a serial interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick et al. the portable device comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector.

Bjorn in analogous art, however, teaches a device comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector. (Col. 2, lines 59-60; the digital connection is a data bus, which conforms to a universal serial bus (USB) standard.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick et al. to include a device comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform

via the USB connector. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Bjorn, in order to provide a faster transfer of digitized image.

5. Claims 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. United States Letters Patent No. 6,088,802 and in view of Estakhri et al. (hereinafter Estakhri) United States Letters Patent No. 6,385,667.

As per claim 23:

Bialick teaches a unitary portable data storage device having biometrics capability the device comprising:

housing; (Figure 3a)

a fingerprint module, at least a portion of which is housed within the housing, the fingerprint module including a sensor disposed on an exterior surface of the housing; (Col. 14, lines 21-67)

a memory including non-volatile memory, the memory housed within the housing and coupled to the fingerprint module and is configured to store at least one fingerprint template as well as user data**; (**Figure 8, item 803; Col. 14; lines 10-58 and Col. 16, lines 10-15)

a memory controller housed within the housing and coupled to the memory, the memory controller controlling access to the memory; (Figure 8, item 801)

wherein the fingerprint module is configured to (1) receive a fingerprint sample from a user placing a finger on the sensor; (Col. 14, lines 55-56) (2) compare the fingerprint sample with said at least one finger template; (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16) and (3) reject a request from the user to access the user data stored in the

memory provided that the comparison in said step (2) results in no match. (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

In addition, Bialick et al. disclose a communication interfaces, such as a smart card interface, a serial interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick et al. a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer and a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol.

Estakhri in analogous art, however, teaches a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer; (Figure 3, element 300, element 314). and a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol. (Figure 3, element 300, element 314, element 335, element 330; Col. 5, lines 19-51)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick et al. to include a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer and a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol. This modification would have been obvious because a person having ordinary skill in the art would have been

motivated to do so, as suggested by Estakhri, (Col. 1, lines 16-17) in order to provide an interface facilitating user-friendly connectivity and a faster transfer of digitized image.

As per claim 24:

Bialick and Estakhri disclose all the subject matter as discussed above. In addition Estakhri further discloses a device wherein at least a portion of the USB plug protrudes from the housing to facilitate direct coupling of the unitary portable data storage device to the USB socket of a computer. (Figure 3, item 314)

(10) Response to Argument

With respect to claim 1:

Appellant's argued that Bialick does not disclose that "*an access code entered via a biometrics-based device can enable access to data stored in a memory of the peripheral device*." , In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "enable access stored in a memory of the peripheral device", "storing data in a memory of the peripheral device", *"an access code has to be entered before a user is enabled to access data stored in a non-volatile memory of a portable device"*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Examiner would like to point out that Bialick discloses a peripheral device which is portable with a processor (figure 8, item 801) a first memory device can be a non-volatile data storage device, (figure 8, item 803) and a second memory device that can be a volatile data

storage device (figure 8, item 804). Bialick teaches that ***a user must successfully enter an acceptable access code (biometrics), not only to control access to the security or other functionality of the peripheral device, but also to identify a "personality" of the user that is stored in the memory of the peripheral devicer.*** (col. 10, lines 52-65) Upon receipt of an acceptable access code, the peripheral device driver can also access and retrieve the data representing the corresponding personality so that the operation of the device can be controlled accordingly ...**enabling a user to perform any functionality (which includes a non-volatile storage of data) that is provided by the peripheral device. (col. 11, lines 16-25) or to access the memory device of the peripheral device (which comprises the non-volatile, Flash 803 and volatile, RAM).** Therefore any functionality of the peripheral device or access to the memory device (access to non-volatile memory) is enabled only after a user successfully enters an access code (i.e. biometrics) otherwise the user is denied access to the peripheral device is an adequate support to meet the claimed limitation, *"access to the non-volatile memory is granted to the user provided that the biometrics-based authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise."*

With respect to claims 7 and 17:

Appellant argued that "*the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module*." Bialick teaches data representing personalities and appropriate access code can be stored in a memory device of the peripheral device. (col. 11, lines 7-10***). Bialick does not exclude that the data representing personalities and corresponding user access codes can be stored in flash memory of the peripheral device. Therefore, the data can be stored in any***

part of the memory device of the peripheral device including the non-volatile memory device (item 803). An access code (biometrics) is used not only to control access to the security and other functionality but also to identify a "personality" of the user that is stored in a memory of the peripheral device. ***Upon receipt of an acceptable access code, the peripheral device driver can also access and retrieve the data representing the corresponding personality so that the operation of the device can be controlled accordingly …enabling a user to perform any functionality that is provided by the peripheral device. (col. 11, lines 16-25)***

In addition, Bialick also discloses that once an acceptable access code has been entered (**i.e. authentication using biometrics**), the user is enabled to select one of the three modes which include target functionality (i.e. non-volatile storage of data …which can be a compact flash memory device). An acceptable access code (i.e. **biometrics**) has to be entered to enable user to select one of the three modes which includes a target functionality (i.e. to store data in compact flash memory; col. 13, lines 27-49). Figure 7 of Bialick specifically discloses the steps, at step 704 the system checks if user has entered appropriate access code and/or identification code. (col. 12, lines 27-28; i.e. biometrics) If the result is yes, at step 705, the user is given option to select one of the three modes of operation (i.e. only security functionality, both security functionality and target functionality and only target functionality). The target functionality includes a memory to enable non-volatile storage of data (col. 13, lines 28-30, *i.e. non-volatile memory*). Then at step 707 if target functionality is embodied as a memory device, the interface can enable the user to specify a name for the stored data. (col. 11, lines 58-60; *i.e. allow access to non-volatile memory*). If the result at step 704 is no (**i.e. proper access code has not been entered**) the process ends without allowing any access to the peripheral device. (see figure 7 below; i.e. *access is denied otherwise*)

Appellant argued that Bialick does not disclose *"a microprocessor that controls a biometrics-based authentication module.... the cryptographic processing device 801 of Bialick is a special microprocessor for performing cryptographic operations. A biometrics-based authentication is not a cryptographic operation."* The Examiner respectfully disagrees. Bialick discloses user authentication can be accomplished by using a biometric data from a user and comparing the biometric data to an appropriate library of biometric data representing a predetermined group of people (e.g. authorized users). The library data can be stored in a memory device of the peripheral device. (col. 14, lines 53-58) The interface control device mediates the interaction between the target functionality and the cryptographic processing device. (figure 8; col. 16, lines 40-43) ***A biometrics-authentication module is used to implement user authentication which is one of the security functionality as disclosed by Bialick (col. 12, lines 31-32)*** Security operations including, for example one or more of the basic cryptographic functions, such as maintenance of data confidentiality, verification of data integrity, user authentication and user non-repudiation. (col. 5, lines 25-29) Since user authentication and user non-repudiation is one of the security operations, the CPU (figure 8, item 801) in the peripheral device compares and verifies the acquired biometrics data with the library of biometric data of authorized users stored in a memory device of the peripheral device in order to authenticate users. Therefore, Bialik teaches a biometric-based authentication device controlled by the microcontroller (i.e. **cpu that performs user authentication,** see figure 8, item 801)

Appellant argued that Bialick does not disclose *"the cryptographic processing device 801 is configured to disable access to a non-volatile memory upon a determination of an authentication failure by a biometrics-based authentication module."* Examiner respectfully disagrees. As pointed

out in discussion above, security operations of the cryptographic processor includes user authentication and if the user has not entered a proper access code (such as biometrics) and authenticated the user is not able to access the non-volatile memory or any other functionality of the peripheral device and the process ends without allowing any access to the peripheral device. (see Figure 7, step 704 and 718)

With respect to claims 4 and 10:

Appellant argued that Bialick does not disclose "*a biometrics sensor being fitted on one surface of a portable device or a biometrics-based authentication module being structurally integrated with a portable device in a unitary construction.*" The Examiner respectfully disagrees. Bialick teaches that the peripheral device is embodied **as a card that can be inserted into a corresponding slot formed in a portable computer** that includes security functionality , target functionality and a host interface that are formed in a single, card-like housing (i.e. unitary construction) conforming to PCMCIA card or smart card standard. (col. 5, lines 40-57) Target functionality of the peripheral device as a biometric device is adapted to receive input data regarding a physical characteristics of a person based upon a physical interaction with the device (col. 14, lines 10-15). Bialick teaches when a peripheral device including fingerprint scanning device is embodied as a card adapted to be inserted into a slot of a host computing device, it may be useful to make the peripheral device relatively long, so that **a portion of the card on which the sensor is positioned can extend from the slot of the host computing device, thereby enabling fingerprints to be scanned while the peripheral device is inserted in host computing device.** (col. 14, lines 59-67) A biometrics sensor on a portion of the card that extends

from the slot is an adequate to meet the claimed limitation "a biometrics sensor fitted on one surface of the portable device. "

With respect to claims 5 and 11:

Appellant argued that Bialick does not disclose "*a non-volatile memory comprising flash memory*." The Examiner respectfully disagrees. Bialick teaches a memory device can be non-volatile data storage device. (see figure 8, item 803) Furthermore, Bialick teaches that target functionality can be embodied as a memory device adapted **to enable non-volatile storage of data**. More particularly, a solid-state storage disk storage devices (e.g. **NAN flash memory device**) can be used. A memory can be **a compact flash memory device**, such as an ATA format flash disk drive. (col. 13, lines 28-37)

With respect to claims 13:

Appellant argued that Bialick does not disclose "*a microprocessor that is configured to direct biometrics-based authentication module to capture and store a first biometrics marker."* The Examiner respectfully disagrees. Bialick discloses user authentication can be accomplished by **using a biometric data from a user and comparing the biometric data to an appropriate library of biometric data representing a predetermined group of people (e.g. authorized users).** The library data can be stored in a memory device of the peripheral device. (col. 14, lines 53-58) The interface control device mediates the interaction between the target functionality and the cryptographic processing device. (figure 8; col. 16, lines 40-43) Bialick teaches that security operations including, for example one or more of the basic cryptographic functions, such as maintenance of data confidentiality, verification of data integrity, **user authentication and user non-repudiation**. (col. 5, lines 25-29) Since user authentication and user non-repudiation is one of

the security operations, the CPU (figure 8, item 801) in the peripheral device compares and verifies the biometrics data and authenticates the user (**which is performed by comparing acquired biometric data with library of biometric data of authorized users**). Therefore, Bialik teaches a biometric-based authentication device controlled by the microcontroller (i.e. **cpu that performs user authentication,** see figure 8, item 801)

With respect to claim 14:

Appellant argued that Bialick does not teach "*a microprocessor configured to enable access to non-volatile memory upon a determination of authentication success by a biometric-based authentication module.*" Bialick teaches a peripheral device that includes a processing device (figure 8, item 801), flash memory (figure 8, item 803) and RAM (figure 8, item 804). Bialick teaches data representing personalities and corresponding user access codes can be stored in a memory device of the peripheral device. An access code (including a biometrics–based authentication) can be used not only to control access to the security functionality but also to identify a "personality" of the user that is stored in a memory of the peripheral device. Once an acceptable access code has been entered (**i.e. authentication using biometrics**), the user is enabled to select one of the three modes which includes target functionality (i.e. a memory adapted to enable non-volatile storage of data …which can be a compact flash memory device). Therefore, the fact that Bialick discloses an acceptable access code (**including biometric-based authentication**) has to be entered to enable user to select one of the three modes which includes a target functionality (i.e. to store data in compact flash memory; col. 13, lines 27-49) meet the claimed limitation access to the non-volatile memory (i.e. a memory for non-volatile storage of data) is granted to the user only if the biometric-based authentication module authenticates the

user's identity and wherein access to the non-volatile memory is denied to the user otherwise access is denied is an adequate support to meet the claimed limitation disabling or denying user access to the non-volatile memory upon a failure of by the biometrics-based authentication module.

With respect to claims 6, 16 and 22:

Appellant argued that Bialick does not disclose "*a microprocessor that provides a bypass mechanism from authentication when authentication of biometrics based authentication module fails. Bialick does not explicitly teach the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.*" Bialick teaches it can be desirable to require an access code before the user is enabled to use the peripheral device. In particular, it can be desirable to require an access code before enabling a user to use the security functionality, thus establishing a layer of security that protects the integrity of the security operations themselves. An access code can be entered in a conventional manner using a user interface device or using a particular embodiment of target functionality such as biometrics device. (col. 10, lines 40-61) Furthermore, Bialick teaches that the **peripheral device assumes target functionality without the security functionality thereby the need for security operations is reduced or eliminated, making implementation and use of data security system including the peripheral device simpler and easier. The possibility that a user will use the system incorrectly (e.g. apply fail to apply security operations incorrectly or incompletely) is reduced** (col. 8, lines 15-36) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Bialick to include a microprocessor that is configured to provide a bypass

mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick, in order to provide a system that allows access to the peripheral device without biometric-based authentication in the event that the user incorrectly or incompletely applies security operations. (Bialick, col. 8, lines 33-37)

With respect to claims 12 and 19:

Appellant argued that Bialick does not teach or suggest *"performing any type of security functionality, such as cryptographic operations, on a biometrics marker that is to be stored in a non-volatile memory of a peripheral device."* Bialick teaches data representing personalities and corresponding user access codes can be stored in a memory device of the peripheral device, access is allowed only after an appropriate access has been entered by the user. User authentication can be accomplished by using a biometric data from a user and comparing the biometric data to an appropriate library of biometric data representing a predetermined group of people (e.g. authorized users). The library data can be stored in a memory device of the peripheral device. (col. 14, lines 53-58) The interface control device mediates the interaction between the target functionality and the cryptographic processing device. (figure 8; col. 16, lines 40-43) Furthermore, Bialick teaches that **it may be desirable to ensure that unencrypted data cannot be transferred via the communication device or stored in the memory device, whether done inadvertently or on purpose. (col. 10, lines 33-36) Since the library data can be stored in a memory device of the peripheral device, the library data (i.e. biometrics data) has be stored in an encrypted format. (col. 14, lines 53-58)** Bialick suggests that data cannot be stored in the

memory device of the peripheral device unencrypted which includes the library of biometrics marker. Therfore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Bialick in order to enhance the security of the library of biometrics data stored in the peripheral device.

With respect to claims 3 and 9:

Appellant argued that "*Bjorn does not teach or suggest directly coupling a USB plug of a portable device having a non-volatile memory to a USB of a USB-compliant device.*" Examiner respectfully disagrees. Bialick teaches that the peripheral device is embodied as a card that can be inserted into a corresponding slot (**i.e. directly coupling**) formed in a portable computer that includes security functionality , target functionality and a host interface that are formed in a single, card-like housing (**i.e. unitary construction**) conforming to PCMCIA card or smart card standard. (col. 5, lines 40-57) Bialick teaches a communication interfaces, such as a smart card interface, a serial interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick is that the portable device, further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device. Bjorn in analogous art, however, teaches a device further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device. (Col. 2, lines 59-60; the digital connection is a data bus, which conforms to a universal serial bus (USB) standard.)

With respect to claim 23:

Appellant argued that Estakhri does not teach "*a USB plug integrated into the housing of a portable memory device without an intervening cable. Rather Estakhri teaches an interface system that has a 50-pin connection as a second end for connection to a removable memory card and has*

a first end to couple the interface system to a host computer. Estakhri merely teaches that the first end of the interface system is configured for coupling to a host computer system, but does not disclose how this coupling is achieved." Bialick teaches that the peripheral device is embodied as a card that can be inserted into a corresponding slot (**i.e. directly coupling**) formed in a portable computer that includes security functionality , target functionality and a host interface that are formed in a single, card-like housing (**i.e. unitary construction**) conforming to PCMCIA card or smart card standard. (col. 5, lines 40-57) with a communication interfaces, such **as a smart card interface, a serial interface or a SCSI interface or an IDE interface.** The peripheral device can be embodied in a card or disk (e.g. a card conforming to a PCMCIA form factor as established by the appropriate standard that is **inserted into a corresponding socket formed in the host computing device.** (col. 6, line 65-col. 7, line 2) which is adequate to meet the claimed limitation "coupling the unitary portable storage device directly to a host computer without an intervening cable." (**i.e. a peripheral device inserted into a corresponding socket in the host computer**) Although Bialick teaches different conforming standards did not explicitly disclose a USB plug a USB plug capable of coupling to a USB socket on a host computer. Estakhri teaches **a flash memory card with enhanced operating mode detection that can be used with different interfaces such as Universal Serial mode, PCMCIA, and ATAIDE mode.** The interface device can be implemented in a variety of protocols that are known to those skilled in the art. The protocols: **Universal Serial Bus (USB), PCMCIA, and ATAIDE** are only few examples for attaching and accessing peripheral devices to the host computer system. (Abstract; col. 5, lines 32-51)

In response to appellant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, one ordinary skill in the art at the time the invention was made would have been motivated to modify the peripheral device disclosed by Bialick to include ***USB plug capable of coupling to a USB socket on a host computer in order to provide a fast bi-directional isochronous transfer of data between external peripheral device and the host computer system at a very low cost as suggested by Estakhri (col. 5, lines 41-43)***.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Shewaye Gelagay

/S. G./

Examiner, Art Unit 2137

Conferees:

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136